



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,928	03/31/2000	Ulhas S Warrior	10559-148001/P7973	2224

20985 7590 05/14/2004

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 05/14/2004

7

Please find below and/or attached an Office communication concerning this application or proceeding.

2

Office Action Summary

Application No.

09/539,928

Applicant(s)

WARRIER ET AL.

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 March 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) 4, 5, and 24 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed on 4 March 2004.
2. Claims 1-3, 6-23, and 25-29 are currently pending in this application. Claims 4, 5, and 24 have been withdrawn. Claims 1, 17, and 21 are independent claims.
3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 25 recites the limitation "the network stack" in the 2nd line of the claim.

There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 1-3, 7-13, 16, 17, 20, and 26-29** are rejected under 35 U.S.C. 102(e) as being anticipated by Flint et al. U.S. Patent No. 6,453,419 (hereinafter '419).

As to independent claim 1 (Currently amended), "A method of managing a network session" is taught in '419 col. 2, line 11-13;

"delivering security policies" is shown in '419 col. 2, lines 6-11 (i.e. "delivering" same as "providing");

“from a server to a remote system that has predetermined configuration information” is disclosed in ‘419 col. 3, lines 3-7;

“and allows running at least one application program” is taught in ‘419 col. 4, lines 17-26 (i.e. “Also included are the system calls that the user level programs need to use the ACLs”);

“establishing a secure virtual private network connection between the server and the system” is shown in ‘419 col. 3, lines 13-25;

“regulating activities in the system based on both of the security policies and a context of said at least one application program including at least a state of running of said at least one application program” is disclosed in ‘419 col. 4, lines 14-26.

As to dependent claim 2 (Currently amended), “wherein said regulating the activities comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria that are conditioned on said running state” is taught in ‘419 col. 5, lines 1-4, (i.e. “running state” same as “Java or ActiveX content”).

As to dependent claim 3 (Currently amended), “wherein the rejection criteria include the predetermined configuration information” is shown in ‘419 col. 2, lines 29-33.

As to dependent claim 7, “further comprising updating the set of policies” is disclosed in ‘419 col. 4, lines 16-18.

As to dependent claim 8, “further comprising: detecting data packets from the regulated activities; and rejecting the data packets from the regulated activities” is taught in ‘419 col. 3 lines 48-53.

As to independent claim 9 (Currently amended), this is directed to a computer readable medium of the method of claim 1 and is rejected along the same rationale.

As to dependent claims 10-13 and 16, these claims contain substantially similar text as claim 2, 3, 7, and 8 above and are rejected along the same rationale.

As to independent claim 17 (Currently amended), this claim is directed toward a network system of the method of claim 1 and is rejected along the same rationale.

As to dependent claim 26, “wherein said policies include information about authorized kinds of information when certain applications are running, and said regulating activities comprises determining if a specified application is running, allowing a specified kind of network packet to pass only when said specified application is running, and blocking said specified kind of network packet from passing when said specified application is not running” is taught in ‘419 col. 4, line 61 through col. 5, line 4 (i.e. “when certain applications are running” same as “filters to block particular WWW connections”) (i.e. “when if a specified application is running” same as “filter node 72 can force user authentication or encryption”).

As to dependent claim 27, “wherein said specified application is a word processing program, and said kind of network packet is word processing data” is shown in ‘419 col. 6, lines 3-11 (i.e. “word processing program” same as “email”).

As to dependent claims 28 and 29, these claims are substantially similar to claim 26 above and are rejected along the same rationale.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. **Claim 6, 14, 15, and 18-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over '419 as applied to independent claim 1 and 17 above, in view of Green et al., U.S. Patent No. 6,003,084 (hereinafter '84).

As to dependent claims 6, "wherein regulating the activities comprises: providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies" is disclosed in '419 col. 5, lines 1-4 "In one embodiment, filter node 72 can force user authentication or encryption, can use filters to block particular WWW connections or can filter the connection to see if it contains Java or ActiveX content"; the following is not taught in '419:

"wherein regulating the activities comprises: providing a session layer adapted to reject unauthorized data packets based on context information" however '84 teaches "with layers 5 and 6 being implicitly provided by the TCP ... If a

Art Unit: 2134

security violation is detected, a meaningful application specific protocol response can be created from context information captured during the session” in col. 2, lines 10-18;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system, and method of implementing an access control mechanism to maintain security in a computer network that also utilizes VPN taught in ‘419 to include a means to address OSI protocol layer structure. One of ordinary skill in the art would have been motivated to perform such a modification to because of the network security needed when utilizing the Internet see ‘084 (col. 2, lines 44 et seq.) “One suite of protocols used by application entities to exchange data is called Open Systems Interconnect (OSI)”.

As to dependent claim 14 and 15, these claims contain text that is substantially similar to claim 6 above and are rejected along the same rationale.

As to dependent claim 18, “further comprising a network stack” is taught in ‘084 col. 5, lines 36-39 “The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports”

As to dependent claim 19, “wherein the network stack comprises: a policy engine connected to the first device; a policy store connected to the policy engine” is shown in ‘84 col. 5, lines 36-39 “The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy

interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports”

“a socket interceptor connected to the policy engine” is disclosed in ‘419 col. 3, lines 48-53 “For each connection attempt, the Firewall checks it against the defined access rules. The rule that matches the characteristics of the connection request is used to determine whether the connection should be allowed or denied.”

“a packet guard connected to the policy engine” is disclosed in ‘419 col. 5, lines 1-4 “In one embodiment, filter node 72 can force user authentication or encryption, can use filters to block particular WWW connections or can filter the connection to see if it contains Java or ActiveX content”.

As to dependent claim 20, “the first device further comprising instruction to monitor the system for the intervening process” is disclosed in ‘084 col. 5 lines 36-39 “The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports”.

9. **Claims 21-23, and 25** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘419 in further view of ‘084, in further view of Cunningham et al., U.S. Patent No. 6,219,786 (hereinafter ‘786), in further view of Trcka et al., U.S. Patent No. 6,453,345 (hereinafter ‘345).

As to independent claim 21 (Currently amended), “A network stack” is taught in ‘084 col. 5 lines 36-39 “The proxy comprises a computer program having a

connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports”

“comprising: a policy engine” is disclosed in '084 col. 5 lines 36-39 “The proxy comprises a computer program having a connection manager portion and a security manager portion. The proxy interfaces with networking software to direct a communication stack to monitor connection requests to any address on specific ports”;

“use the socket interceptor to detect and reject data packets from unauthorized users and applications” is taught in '419 col. 5, lines 1-4 “In one embodiment, filter node 72 can force user authentication or encryption, can use filter to block particular WWW connections, or can filter the connection to see if it contains Java or ActiveX content”;

“use the packet guard to filter unauthorized activities received from the network interface; use the packet guard to filter the data packets from unauthorized users and applications based on the context information received by the socket interceptor; and use the packet guard to filter data packets based on the policies” is shown in '419 col. 5, lines 1-4 “In one embodiment, filter node 72 can force user authentication or encryption, can use filter to block particular WWW connections, or can filter the connection to see if it contains Java or ActiveX content”;

the following was not taught in the combination of teachings from '419 and '084:

“a policy store adapted to interact with the policy engine and store a set of policies from the policy engine; ” is disclosed in ‘786 col. 4 lines 13-17 “the access rules are preferably stored as a rules base, which may be centralized if there is more than one node that provides access management. Alternatively, the rules base is configured at a single site, but then automatically distributed to each access control point on the network”;

“a socket interceptor coupled to the policy engine” is shown in ‘786 col. 1, lines 54-56 “These gateways are “choke points, through which network traffic that is to be controlled must flow” and ‘786 col. 6, lines 8-9 “an access control module 34 is installed on the firewall 16 in order to form a gateway access control station (GACS)”

“a packet guard coupled to the policy engine” is disclosed in ‘786 col. 3 lines 21- 34 “access control to resources of a network by collecting and assembling data packets of a specific transmission, so as to enable identification of information from raw data packets at the lowest level to application-level data at the top-most level. In terms of the standardized model referred to as the International Standards Organization (ISO) model, the data packets are assembled to determine not only the lower-layer information from the headers of the packets, but also the uppermost Application Layer (i.e., Layer 7) contextual information. Access rules are then applied to determine whether the specific transmission is a restricted transmission”;

“a configurable management process adapted to reconfigure the network stack and having instructions to:” is taught in ‘786 col. 6, lines 16-20 “The access control modules 30, 32 and 34 can be installed, de-installed, and reinstalled on any of

the nodes of the network at any time to suit potentially changing network topologies or changing access management policies”;

“receive policies in the policy engine from the policy server” is shown in ‘786 col. 6, lines 49-53 “After a rules base has been configured by a system operator, the rules base is downloaded to the access control modules 30, 32 and 34. Thus, any subsequent changes in the rules base may be implemented at the various nodes in an efficient dynamic manner”;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system, and method of implementing an access control mechanism to maintain security in a computer network that also utilizes VPN and OSI protocol layer structure taught in the combination of ‘419 and ‘084 to include a means to maintain a policy store. One of ordinary skill in the art would have been motivated to perform such a modification because a policy store maintains the flexibility of the network see ‘786 (col. 3 lines 16 et seq.) “What is needed is a method and system for providing access control to resources of a network in a manner that is flexible, scalable and relatively easy to administer”.

The following is not taught in the combination of teachings of ‘419, ‘084, and ‘786:

“and provide the packet guard with context information about the unauthorized users and applications including at least information about a running state of the application” however is taught in “The information captured by such WAN-side monitoring following a break-in may be useful, for example, for

Art Unit: 2134

identifying the intruder or for determining the "flaw" in the company firewall that enabled the intruder to gain access" '345 col. 8, lines 37-56.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system, and method of implementing an access control mechanism to maintain security in a computer network that also utilizes VPN, OSI protocol layer structure, and a policy store taught in the combination of '419, '084, and '786 to include a means to identify events at the packet level. One of ordinary skill in the art would have been motivated to perform such a modification to protect a network against unknown attacks see '345 (col. 1 lines 53 et seq.) "One problem with existing firewall systems is that they are generally only effective at protecting against known types of security attacks".

As to dependent claim 22, "The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard" is disclosed in '786 col. 2 lines 58-63 "By monitoring all packets, the system detects occurrences in which a device attempts to "disguise" itself by first training with an authorized source address and then sending a packet with an unauthorized source address."

As to dependent claim 23, "The network stack of claim 21 further comprising an interface to a network adapted to connect the network stack to the network, wherein the network has a policy server" is disclosed in '786 col. 4 lines 13-17 "the access rules are preferably stored as a rules base, which may be centralized if there is more than one node that provides access management. Alternatively, the

rules base is configured at a single site, but then automatically distributed to each access control point on the network.”

As to dependent claim 25, “wherein said regulating activities comprises reconfiguring the network stack to control filtering of network packets, based on said policies and said running state” is taught in ‘786 col. 6, lines 16-20 “The access control modules 30, 32 and 34 can be installed, de-installed, and reinstalled on any of the nodes of the network at any time to suit potentially changing network topologies or changing access management policies”.

Response to Arguments

10. Applicant's arguments filed 4 March 2004 have been fully considered but they are not persuasive.

In response to applicants argument on page 11 that a “virtual private network connection, which by itself distinguishes over Flint ... subject matter of amended claim 1 is not in any way taught or suggest by the cited prior art” applicant is incorrect a virtual private connection was indicated in Flint col. 4, lines 15-30.

In response to applicant's argument on page 12, “An important feature of the present system is the way the client gets policies” this is taught in the main reference in which access control is maintained through workstations through and internal and external network connections (see col. 3, lines 3-30).

In response to applicant's argument on page 12 “activities are regulated based on the security policies and context of at least one application program” this is shown in Flint filters can be applied at any point in an access rule. (see ‘419 col. 4, lines 50-67).

In response to applicant's argument on page 13, "There is nothing teaching or suggesting, however that the packet blocking is based not only on the access rules, but also the running state of an application" applicant is incorrect this has been rejected in the above claims, i.e. a user utilizing the Internet is a "running application" blocking certain cites or subject emails is the same as "blocking ... the running state" (see col. 6, lines 3-11).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

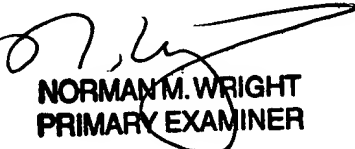
11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm Monday - Thursday and alternating Fridays.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Ellen. Tran
Patent Examiner
Technology Center 2134
April 16, 2004


NORMAN M. WRIGHT
PRIMARY EXAMINER